(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 March 2001 (01.03.2001)

PCT

(10) International Publication Number
WO 01/14974 A2

(51) International Patent Classification[7]: G06F 12/14

(21) International Application Number: PCT/US00/23028

(22) International Filing Date: 23 August 2000 (23.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/149,910	23 August 1999 (23.08.1999)	US
09/604,727	28 June 2000 (28.06.2000)	US

(71) Applicant: **PRESIDEO, INC.** [US/US]; 10305 102nd Terrace, Sebastian, FL 32958 (US).

(72) Inventors: **SCHWEITZER, Shelia, H.**; 171 Shores Drive, Indian River Shores, FL 32963 (US). **LOWTHERS, Bruce, F., Jr.**; 5280-402 W. Harbor Village Drive, Vero Beach, FL 32967 (US). **HOFFMAN, Thomas, C.**; 473 Red Sail Way, Satellite Beach, FL 32937 (US). **FLICKINGER, David, B.**; 1831 Highway A1A #3304, Indian Harbor Beach, FL 32937 (US). **BURKS, James, L.**; 1200 Spanish Lace Lane, Vero Beach, FL 32963 (US).

(74) Agents: GARRET, Arthur, S. et al.; Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P., 1300 I Street, N.W., Washington, DC 20005-3315 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

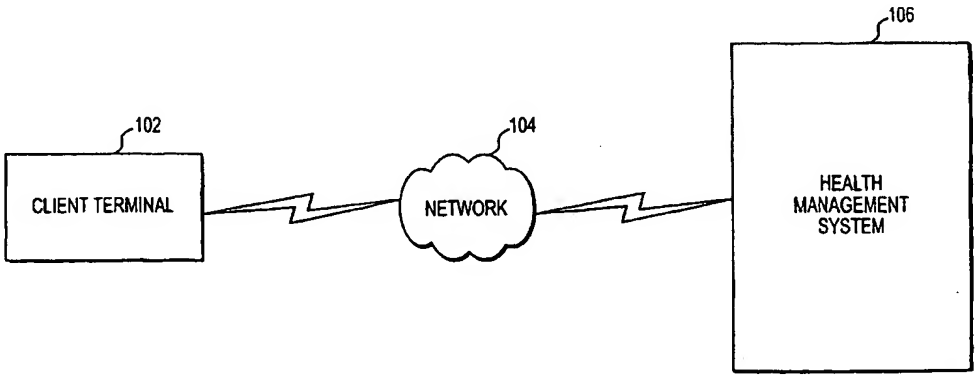
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM, METHOD, AND ARTICLE OF MANUFACTURE FOR IDENTIFYING AN INDIVIDUAL AND MANAGING AN INDIVIDUAL'S HEALTH RECORDS



(57) Abstract: A system, method, and article of manufacture for identifying an individual and managing health records of the individual are provided. The method includes storing health data of an individual on a storage medium. The method also includes logging into the storage medium to manage the health data stored one the storage medium and managing the health data on the storage medium.

WO 01/14974 A2

SYSTEM, METHOD, AND ARTICLE OF MANUFACTURE FOR IDENTIFYING AN INDIVIDUAL AND MANAGING AN INDIVIDUAL'S HEALTH RECORDS

RELATED APPLICATION

The present application claims the benefit of U.S. provisional application no. 60/149,910, filed August 23, 1999, and also is a continuation-in-part of U.S. non-provisional application no. 09/604,727, filed June 28, 2000. The content of all the aforesaid applications are relied upon and expressly incorporated herein by reference.

BACKGROUND OF THE INVENTION

A. Field of the Invention

The present invention relates to the healthcare industry, and more particularly, to a system, method, and article of manufacture for identifying an individual and managing an individual's health records.

B. Description of the Related Art

In the healthcare industry, identifying an individual and managing an individual's health records are important tasks for obvious reasons. For example, in an emergency, a provider, such as a hospital, may need to access an individual's health records to determine if the individual is allergic to a drug. Managing includes, but is not limited to, obtaining, accessing, and updating an individual's records. Identifying an individual and/or managing an individual's health records, however, is difficult, costly, and time-consuming with the currently available mechanisms.

For example, most providers require an individual to complete a lengthy form to obtain personal information, such as payer information, and personal health history or record, a process which is both time-consuming and costly, both for the individual who is seeking health services and for the provider. Moreover, if an individual changes providers, the individual will need to complete another form for the new provider. In addition, in some instances, because of an individual's unfamiliarity with medical terms, an individual may not be able to provide information, such as tests performed, to a new provider. As a result, the new provider may perform a test again, a process which may result in additional costs for the payer, such as an insurance company.

Moreover, in an emergency, as described above, a provider may not be able to quickly access an individual's health records to determine, for example, if the individual is allergic to a particular drug.

Furthermore, in some cases, an individual may fraudulently use a relative's payer card, such as an insurance card, to obtain healthcare services from a provider. Since most providers do not compare an individual's identity with the payer card, an individual may present a relative's payer card to a provider and receive health services from the provider. The provider may charge the payer associated with the payer card for the services rendered and the payer may in turn pay the provider. This results in fraud, which if not detected, may result in additional costs for the payer.

Accordingly, there is presently a need for a system, method, and article of manufacture for identifying an individual and managing an individual's health records easily, quickly, and in a cost-effective manner.

SUMMARY OF THE INVENTION

The present invention provides a method, system, and article of manufacture for identifying an individual and managing health records of the individual. The method includes storing health data of an individual on a storage medium. The method also includes logging into the storage medium to manage the health data stored on the storage medium and managing the health data on the storage medium.

The present invention also includes a system for identifying an individual and managing health records of the individual. The system includes means for storing health data of an individual on a storage medium. The system also includes means for logging into the storage medium to manage the health data stored on the storage medium and means for managing the health data on the storage medium.

Moreover, the present invention provides a computer-readable medium containing instructions for causing a computer to perform a method for identifying an individual and managing health records of the individual. The method includes storing health data of an individual on a storage medium. The method also includes logging into the storage medium to manage the health data stored on the storage medium and managing the health data on the storage medium.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings are incorporated in and constitute a part of this specification and, together with the description, explain the advantages and principles of the invention. In the drawings,

FIG. 1 is a diagram of an exemplary network environment in which features of the present invention may be implemented;

FIG. 2 is an exemplary block diagram illustrating components of the client terminal 102 that is shown in FIG. 1;

FIG. 3 is an exemplary block diagram illustrating components of the health management system 106 that is shown in FIG. 1;

FIG. 4 is an exemplary flowchart illustrating the steps involved in enrolling an individual with a payer plan;;

FIG. 5 is an exemplary flowchart illustrating the steps involved in using a storage medium, such as a card, in accordance with the present invention;

FIG. 6 is an exemplary block diagram illustrating components of a provider terminal; and

FIG. 7 is another diagram of an exemplary network environment in which features of the present invention may be implemented.

DETAILED DESCRIPTION

The following detailed description of the invention refers to the accompanying drawings. While the description includes exemplary embodiments, other embodiments are possible, and changes may be made to the embodiments described without departing from the spirit and scope of the invention. The following detailed description does not limit the invention. Instead, the scope of the invention is defined by the appended claims and their equivalents.

The present invention provides a system, method, and article of manufacture to identify an individual and to manage an individual's health records easily, quickly, and in a cost-effective manner. For example, with the use of the present invention, an individual may store his personal and health information on a storage medium, such as

a smart card. While stored on the card, the information also may be encrypted. The individual may take the card to a provider, who may retrieve or update the information on the card. To retrieve the information, the provider may require the individual to authenticate. Authentication may include, but is not limited to, the use of a biometric and/or a user name and password. Biometric authentication includes the use of unique physical characteristics of a user, such as fingerprint patterns, voice, eyes, face, hand, etc., to confirm the identity of an individual. In addition, the card may be used for other purposes, for example, as a credit card or an access card to enter a building, for example.

The above example is intended to be illustrative of the features of the present invention as opposed to limiting it in any manner. Moreover, the system, method, and article of manufacture are not limited to any particular provider, payer, or individual. A provider is anyone who provides healthcare services and may include, but is not limited to, a doctor, a hospital, a laboratory, or a pharmacy. A payer is anyone who pays for healthcare services, for example, an insurance company. An individual may include, but is not limited to, an employee of an organization. An organization may include, but is not limited to, a business, a government entity, and a non-profit organization.

The above-noted features, other aspects, and principles of the present invention may be implemented in various system or network configurations to provide automated and computational tools to identify an individual and to manage an individual's health records. Such configurations and applications may be specially constructed for performing the various processes and operations of the invention or they may include a general purpose computer or computing platform selectively

activated or reconfigured by program code to provide the necessary functionality. The processes disclosed herein are not inherently related to any particular computer or other apparatus, and may be implemented by a suitable combination of hardware, software, and/or firmware. For example, various general purpose machines may be used with programs written in accordance with teachings of the invention, or it may be more convenient to construct a specialized apparatus or system to perform the required methods and techniques.

The present invention also relates to computer readable media that include program instruction or program code for performing various computer-implemented operations based on the methods and processes of the invention. The media and program instructions may be those specially designed and constructed for the purposes of the invention, or they may be of the kind well-known and available to those having skill in the computer software arts. The media may take many forms including, but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media includes, for example, optical or magnetic disks. Volatile media includes, for example, dynamic memory. Transmission media includes, for example, coaxial cables, copper wire, and fiber optics. Transmission media can also take the form of acoustic or light waves, such as those generated during radio-wave and infra-red data communications. Examples of program instructions include both machine code, such as produced by compiler, and files containing a high level code that can be executed by the computer using an interpreter.

FIG. 1 is a diagram of an exemplary network environment in which features of the present invention may be implemented. The network environment includes client terminal 102 and health management system 106, which are interconnected by

network 104. Network 104 may be a single or a combination of any type of computer network, such as the Internet, an Intranet, an Extranet, a Local Area Network (LAN), or a Wide Area Network (WAN), for example. These as well as other network configurations are known to those skilled in the art and are also within the scope of the present invention. For example, the use of the Internet and specifically, the World Wide Web ("Web") is widely known. The web is a distributed system that includes web servers and web clients. Web servers are software applications that support common protocols, such as Hypertext Transport Protocol (HTTP). Moreover, these web servers make documents, such as documents in hypertext mark up language (HTML), and other resources available to users via web pages. Web clients include software applications, such as a browser, which a user uses to access a web page, for example.

Moreover, while the components of FIG. 1 are shown as logical devices, one skilled in the art would readily understand that each is associated with respective physical devices. For example, client terminal 102 may be a physical device, such as a personal computer, a handheld computer, a laptop, or any similar device known to those skilled in the art.

As shown in FIG. 2, the client terminal 102 may include a browser 210, such as a world wide web browser like NETSCAPE NAVIGATOR and/or INTERNET EXPLORER; other software and data storage 220; at least one input device 230, such as a keyboard or a mouse; at least one communications device 240, such as a modem or a network interface card (NIC); at least one processor 260; memory 250; and at least one output device 270, such as a monitor; all of which may communicate with each other, for example via a communication bus 280. The client terminal 102 also

may include a reading and writing device 290, such as a device for reading and writing to a smart card, and/or a biometric device 295. The biometric device 295 may be, for example, a finger scanner that is used to scan an individual's fingerprint pattern for authentication purposes. The memory 250 may be random access memory (RAM), read only memory, or both. Other client terminals and their components are known to those skilled in the art and are also within the scope of the present invention. For example, it is known to one skilled in the art that in order for the biometric device 295 to interface with the client 102, software drivers may be needed.

Health management system 106 shown in FIG. 1 will be described now. As shown in FIG. 3, the health management system 106 includes a web server 305 and a storage server 335, which are connected to each other via a non-routed network 330, such as a non-routed LAN. The web server 305 includes authentication component 310, certificate component 315, health management component 320, and auditing and reporting component 325. The storage server 335 may include a database 340 and an audit log 345. The data associated with an individual is stored in the database 340. Since, the non-routed network 330 may not be accessed directly from the network 104, such as the Internet, this provides a more secure computing environment because unauthorized individuals will not be able to gain access to the database 335 and audit log 345. Although not shown, both the web server 305 and the storage server 335 also may have an administration component for administering the various components. Moreover, in FIG. 3, the various components are shown to exist on a single web server 305 and a single storage server 335; however, it is known to one skilled in the art that these components may exist on multiple servers to assist in load balancing, for example.

Each of the components shown in FIGs. 1-3 may use various protocols to communicate with each other. In addition, the communication between the various components may be encrypted. For example, the client 102 may communicate with the web server 305, for example, by using the Hypertext Transport Protocol (HTTP) protocol. CORBA's (Common Object Request Broker Architecture) IIOP (Internet Inter-Object Request Broker Protocol) may also be used. Moreover, the secure sockets layer (SSL) also may be used, both as a protocol and encryption. For example, 128 bit SSL encryption may be used. Other encryption algorithms, such as the Blowfish 448-Bit encryption algorithm, may be used. These and other similar protocols and encryption algorithms are known to those skilled in the art and are also within the scope of the present invention.

The components shown in FIG. 3 will be described now. The authentication component 310 performs all authentication related functions. The authentication component 310 is transparent to an individual. The authentication component 310 may use, for example, a user name and authentication token. Authentication token may include any authentication means known to those skilled in the art. For example, authentication token may include a biometric; an access card, such as a smart card; and/or a password. As a result of authentication tokens, such as biometric authentication, the present invention creates a secure computing environment.

The certificate component 315 shown in FIG. 3 will be described now. The certificate component 315 manages certificate issuance and storage. The certificate component 315 is not a certificate authority (CA). Instead, the certificate component 315 may request, renew, revoke and validate standard certificates, such as X.509v3 certificates, through a recognized certificate authority. For example, in FIG. 3,

certificate authority 350 may be used as the certificate authority. All interaction with the certificate authority may be based on, for example, public-key cryptography standards (PKCS) and as a result, the present invention may be compliant with all PKCS compliant certificate authorities. In one embodiment of the present invention, the private key associated with a certificate may be stored on an individual's card, such as a smart card. This allows for greater mobility. The process of storing the private key will be described later.

The auditing and reporting component 325 shown in FIG. 3 will be described now. The auditing and reporting component 325 may provide an interface to all of the other components shown in FIG. 3 in order to provide report information on selected or all data fields. Access to the reports themselves may be audited and restricted to authorized individuals, such as administrators, who have successfully authenticated into the health management system 106. For example, when an individual attempts to access a report, the individual may be required to enter a user name and an authentication token. After the individual provides the requested information and after the information has been verified, the individual may be given access to the report. In one embodiment, the auditing and reporting component 325 may provide e-mail alerts to administrators. These alerts may notify the administrator, for example, of repeated authentication failures.

As described in the foregoing description, the present invention provides an individual with a storage medium, such as a smart card, for use as a payer card. The smart card may have the individual's personal as well as health information stored on it, which may be later retrieved by a provider, for example. Normally, an individual enrolls in a payer plan, such as a health insurance plan, through an enroller. An

enroller may be the individual's employer, a broker, or the payer itself. The process of enrolling with a payer, obtaining a card, and storing information on the card will be described now by referring to FIG. 4.

As indicated by a step 405 in FIG. 4, the enroller, such as an employer or a broker, authorizes an individual to enroll in a payer plan. Next, in a step 410, the enroller establishes an account for the individual in the health management system 106. The account may include a user name and an authentication token, for example. The authentication token may be a password or a biometric. Instead of establishing an individual account, the enroller may assign the same account to all individuals and once logged into the health management system 106, the individuals may be required to establish separate accounts.

Then, in a step 415, the individual uses the account information and client 102 to login to the health management system 106. For example, the individual may use the communications device 240 to connect to the Internet and then, use the browser 210 to go to the web site associated with the health management system 106. The enroller may provide the address of the web site to the individual in step 410, for example. The authentication component 310 may ask the individual to enter account information, such as a user name and an authentication token. Once the individual provides that information, the authentication component 310 may compare this information to the information stored in database 340. The process of establishing accounts and authenticating using a configuration similar to the one shown in FIG. 1 is described in detail in the related U.S. non-provisional application no. 09/604,727, filed June 28, 2000, which is expressly incorporated herein by reference.

After logging into the health management system 106, the health management

component 320 may present web pages, such as a web enrollment form or application, asking the individual for enrollment information, as indicated by a step 420. Some of the enrollment information on the form may be already filled in depending on, for example, whether the enroller established an individual account for the individual. If some or all the enrollment information is already filled in the form, the individual may be asked to verify this information and correct it if necessary. The enrollment information may include, but is not limited to, the individual's name, address, date of birth, social security number, information about spouse and children, information about the payer plan that the individual desires to enroll in, and information about the individual's primary physician and dentist, for example. In addition, the enrollment information may also include employer information if the individual is enrolling through an employer, for example. In step 420, an account, if one already does not exist, may be created for the individual. The account information is stored in the database 340.

Next, in a step 425, the enrollment information is stored in the database 340 and sent to the payer. The information may be sent in a variety of ways. For example, the information may be sent electronically, such as via e-mail, or manually, such as via U.S. mail. If the information is sent electronically, the health management system 106 may generate an e-mail and send it via network 104 to the payer. These and other ways of sending information are known to one skilled in the art and are also within the scope of the present invention.

Upon receipt of the information from the health management system 106, the payer may enroll the individual in the payer plan selected by the individual, as shown in a step 430. Although not shown in FIG. 4, if there are any problems with enrolling

the individual, the payer may contact the enroller, for example, to resolve the problems. After enrolling the individual, the payer may send an acknowledgment to the health management system 106, as indicated by a step 435. The acknowledgment may indicate, for example, acceptance or denial of the individual's application, or may ask for additional information. The acknowledgment may also include the individual's account or identification number that is associated with the payer. This account number may also be stored in the individual's account in the database 340. If the acknowledgment asks for additional information, the additional information may be provided to the payer to complete the enrollment process.

The health management system 106 may be operated and/or owned by a independent third party, enroller, or a payer. For example, if the system 106 is operated by a third party or a payer, the system 106 may send acknowledgment to the enroller, who may in turn send an acknowledgment to the individual, for example, after receiving acknowledgment from the payer. On the other hand, if the system 106 is operated by the enroller, only an acknowledgment to the individual may be necessary.

Once an acknowledgment is received, the health management system 106 may send some or all of the enrollment information, such as the individual's name, and payer information, such as account information and payer name, to a card issuer for issuance of a card. The card may include, but is not limited to, a smart card or a card with a magnetic stripe. In addition, as described in the foregoing description, the card of the present invention may be used for multiple purposes, for example, both as a payer card and a credit card. Consequently, if the card will be used as a credit card also, the enrollment and the payer information may be sent to a credit card issuer in

step 440. If the card also will be used as a credit card, for example, the individual also may need to provide salary information to the credit card company. The use of the card is not limited to a credit card only, other uses will be apparent to one skilled in the art and such uses are also within the scope of the present invention. For example, the card may be used for entry into the individual's employer's building, as a library card, or a copy card. Moreover, the card may be issued by the enroller or the payer.

Next, in a step 445, the card issuer may issue the card to the individual. Although not shown in FIG. 4, if the card issuer needs to verify information or needs additional information, the card issuer may ask for additional information from the health management system 106, for example. The transfer of information between the card issuer may be accomplished in a manner similar to transfer of information between the payer and the health management system 106.

Then, in a step 450, after receiving the card, the individual may login to the health management system 106 using client 102, for example, to activate the card. Once logged in, the individual may select the option of completing the enrollment process, for example, as shown in a step 455. The health management component 320 may present a web page asking the individual for information regarding the individual's health. For example, the component 320 may ask the individual for the individual's health history and information about any drugs that the individual is allergic to. Some or all of the individual's enrollment, payer, and health information may be downloaded to the card in this step for retrieval and update by a provider, for example. In this step, the individual, the enroller, or the payer also may be given the option of selecting the information that needs to be stored on the card and the means of accessing that information. For example, in one embodiment, the individual's

information may be divided and stored on the card in two categories, public and private information. The public information may include, for example, the individual's name and address, etc., whereas the private information may include, for example, payer information and the individual's health history. The public information may be retrieved from the individual's card by just inserting the card in device, such as a reading and writing device. On the other hand, the private information may be stored in an encrypted manner on the card and may be only accessed after authentication. For example, the individual may need to authenticate to the card before the private information may be retrieved.

To provide authentication, the health management component 320 may ask the individual for a user name and an authentication token, for example, which may be stored on the card in step 455. The authentication token may include a biometric or a password, for example. The health management component 320 may ask the individual to place the individual's finger on the biometric device 295. After scanning the individual's fingerprint pattern, the image of the finger may be converted into an authentication token and stored on the card and the database 340. As a result, if a provider, such as a doctor, wants to access the private information, for example, the individual may need to login to his card before the provider can get access to this private information.

In addition to authentication, the private information also may be encrypted. For example, in step 455, the certificate component 315 may request a certificate from the certificate authority 350. Once a certificate is issued, the certificate component 315 may store the private key associated with the certificate on the card and in the database 340. The private key is stored in the database 340 in case the individual

losses his card and a new card needs to be issued to the individual. As a result, when the information is being transferred to the card, some or all of the information, such as the private information, may be encrypted by the private key and then, stored on the card. As a result, if a provider, such as doctor, wants access to the private information, for example, the individual may need to login to his card to retrieve the private key so that the individual's information may be decrypted by using the private key and presented to the provider. Consequently, the present invention secures an individual's personal information and provides access to this information only after authentication by the individual.

Once the information is downloaded on the card, a message may be sent both to the payer and the card issuer, to let them know that the card has been received and to activate the card., as indicated in a step 460. The message may be, for example, digitally signed using the individual's private key. After the message is sent, the individual is ready to use the card, and the enrollment process is complete, as indicated by a step 465. The above process is intended to be illustrative of the features of the present invention as opposed to limiting it in any manner. For example, the steps do not have to be performed in the described order.

An example and FIG. 5 will be used now to describe the process of using a card of the present invention. In this example, it is assumed that an individual desires to visit a provider, such as a doctor. The provider may have a provider terminal similar to the client terminal 102 shown in FIG. 2. The components of a provider terminal 600 are shown in FIG. 6. The components shown in FIG. 6 are similar to FIG. 2 with the exception of the provider component 697. The provider component 697 may be implemented, for example, using software, such as Java applets. In a step

505, the provider component 697 may ask the individual to insert his card into the reading and writing device 690. If the card has public and private information, as described above, the public information will be immediately available to the provider, and the provider may be able to read this information, as shown in a step 510. If the provider does not need any other information, such as the private information, the process may be complete, as indicated by steps 535 and 540.

If, however, the provider wants access to the private information, the provider may ask the individual to authenticate, as indicated by steps 515 and 520. For example, if biometric authentication is being used, the provider component 697 may ask the individual to place his finger, for example, on the biometric device 695. The captured image will be compared to the authentication token stored on the card and if it matches, the provider will be given access to the private information, as indicated by steps 525 and 530. Conversely, if the image does not match, the individual may be asked to try again.

If encryption is also being used, after authentication, the private key may be used to decrypt the private information before presenting it to the provider. The provider may either print and/or transfer the retrieved information to the provider's own system. Once the information has been retrieved, the provider component 697 may instruct the individual to take out his card from the reading and writing device 290 to indicate that the process is complete, as indicated by steps 535 and 540.

In another embodiment, after the provider is finished with the treatment, for example, the provider may update an individual's card, using the provider component 697 and the reading and writing device 290. Updating the individual's card will ensure that current information about the individual's health is stored on the card.

In still another embodiment, as shown in FIG. 7, the provider terminal may be connected to the health management system 106 via network 104, for example. One advantage of this embodiment is that in addition to updating the information on an individual's card, the provider may be able to update the information in the database 340. Another advantage is that if a card has a limited storage space, a provider may be able to access some information from the database 340 after the individual authenticates in addition to the information from the card.

The present invention, as described above, provides several advantages. One advantage is that an individual's health records may be managed easily and quickly. For example, with the present invention, a provider may not need to ask an individual to complete a lengthy form to obtain personal information from the individual because such information can be retrieved from the card. As a result, the provider and the individual save time and costs are reduced..

Another advantage is that since the health information is stored on the card, redundant tests may be reduced. For example, as described in the foregoing description, because of an individual's unfamiliarity with medical terms, an individual may not be able to provide information, such as tests performed, to a new provider. As a result, the new provider may perform a test again, a process which may result in additional costs for the payer, such as an insurance company. With the present invention, however, the new provider will be able to quickly retrieve the individual's health information, including tests performed, from the card if the provider is not connected to the health management system 106 and/or database 340 if the provider is connected to the health management system 106 and thus, may not need to perform tests again even if the individual is unfamiliar with medical terms.

Still another advantage is that in an emergency situation, a provider may be able to quickly access an individual's health information to determine, for example, a drug that an individual is allergic to by using the individual's card. This is possible as long as the information is stored on the card as public information. Moreover, even private information may be accessed, for example, by giving a family member of the individual access to the private information. Access may be given, for example, by placing the authentication token of the individual's family member in addition to placing the authentication token of the individual on the card. These and other methods of accessing information from the card will be apparent to one skilled in the art and are also within the scope of the present invention.

Yet another advantage of the present invention is that it identifies the individual and reduces fraud. For example, with the present invention, an individual may not use a relative's payer card to obtain healthcare services from a provider because the present invention may require an individual to authenticate to the individual's card before any information can be retrieved from it. As a result, unless the individual provides his information to someone else, fraud is unlikely. Moreover, if biometric authentication is used, the individual will need to authenticate by himself and cannot provide such information to another.

Still another advantage of the present invention is that an individual may use the card for other purposes, such as a credit card or a library card. Furthermore, another advantage is that if an individual losses his card or a provider losses the individual's records, the individual may be able to quickly obtain a new card and the provider may be able to quickly obtain a copy of the records by using the health management system 106.

While the examples given in the foregoing description related to an individual, the present invention is not limited to the individual. For example, the present invention may be used in a similar manner for the individual's family members, such as a spouse.

It will be apparent to those skilled in the art that various modifications and variations can be made in the system and method of the present invention and in construction of this invention without departing from the scope or spirit of the invention.

Moreover, other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the invention being indicated by the following claims.

WHAT IS CLAIMED IS:

1. A method for identifying an individual and managing health records of the individual, comprising the steps of:

storing health data of an individual on a storage medium,

logging into the storage medium to manage the health data stored on the storage medium; and

managing the health data on the storage medium.

2. The method of claim 1, further comprising the step of storing a private key associated with a certificate of the individual on the storage medium.

3. The method of claim 2, wherein the health data includes public and private health data.

4. The method of claim 3, wherein the step of storing health data of an individual on a storage medium includes the step of encrypting the private health data with the private key.

5. The method of claim 4, wherein the step of managing includes decrypting the private health data with the private key.

6. The method of claim 1, wherein the step of logging into the storage medium to manage the health data stored on the storage medium includes the steps of:

receiving authentication data from the individual;

comparing authentication data received from the individual with authentication data stored on the storage medium; and

ensuring that the authentication data received from the individual matches with authentication data stored on the storage medium.

7. The method of claim 6, wherein the authentication data may be chosen from user name and password and user name and biometric.

8. The method of claim 1, wherein the step of managing includes accessing and updating the health data.

9. A system for identifying an individual and managing health records of the individual, comprising:

means for storing health data of an individual on a storage medium,

means for logging into the storage medium to manage the health data stored on the storage medium; and

means for managing the health data on the storage medium.

10. The system of claim 9, further comprising means for storing a private key associated with a certificate of the individual on the storage medium.

11. The system of claim 10, wherein the health data includes public and private health data.

12. The system of claim 11, wherein the means for storing health data of an individual on a storage medium includes encrypting the private health data with the private key.

13. A computer-readable medium containing instructions for causing a computer to perform a method for identifying an individual and managing health records of the individual, comprising the steps of:

storing health data of an individual on a storage medium,

logging into the storage medium to manage the health data stored on the storage medium; and

managing the health data on the storage medium.

14. The computer-readable medium of claim 13, further comprising the step of storing a private key associated with a certificate of the individual on the storage medium.

15. The computer-readable medium of claim 14, wherein the health data includes public and private health data.

16. The computer-readable medium of claim 15, wherein the step of storing health data of an individual on a storage medium includes the step of encrypting the private health data with the private key.

17. The computer-readable medium of claim 16, wherein the step of

managing includes decrypting the private health data with the private key.

18. The computer-readable medium of claim 13, wherein the step of logging into the storage medium to manage the health data stored on the storage medium includes the steps of:

receiving authentication data from the individual;

comparing authentication data received from the individual with authentication data stored on the storage medium; and

ensuring that the authentication data received from the individual matches with authentication data stored on the storage medium.

19. The computer-readable medium of claim 18, wherein the authentication data may be chosen from user name and password and user name and biometric.

20. The computer-readable medium of claim 13, wherein the step of managing includes accessing and updating the health data.

21. The method of claim 1, wherein the storage medium is chosen from a smart card and a magnetic stripe card.

22. The method of claim 21, wherein the storage medium may be used as a credit card.

23. The system of claim 9, wherein the storage medium is chosen from a smart card and a magnetic stripe card.

24. The system of claim 23, wherein the storage medium may be used as a credit card.

25. The computer-readable medium of claim 13, wherein the storage medium is chosen from a smart card and a magnetic stripe card.

26. The computer-readable medium of claim 25, wherein the storage medium may be used as a credit card.

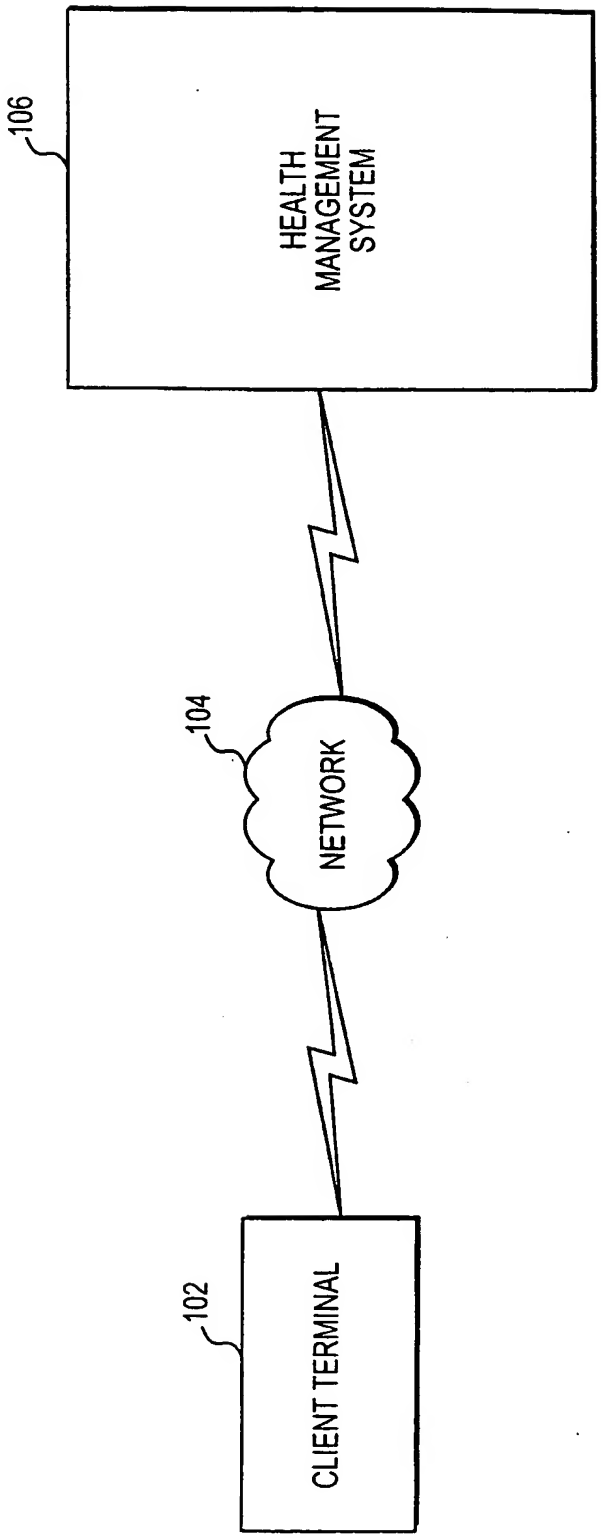

106
HEALTH MANAGEMENT SYSTEM
104
NETWORK
102
CLIENT TERMINAL

FIG. 1

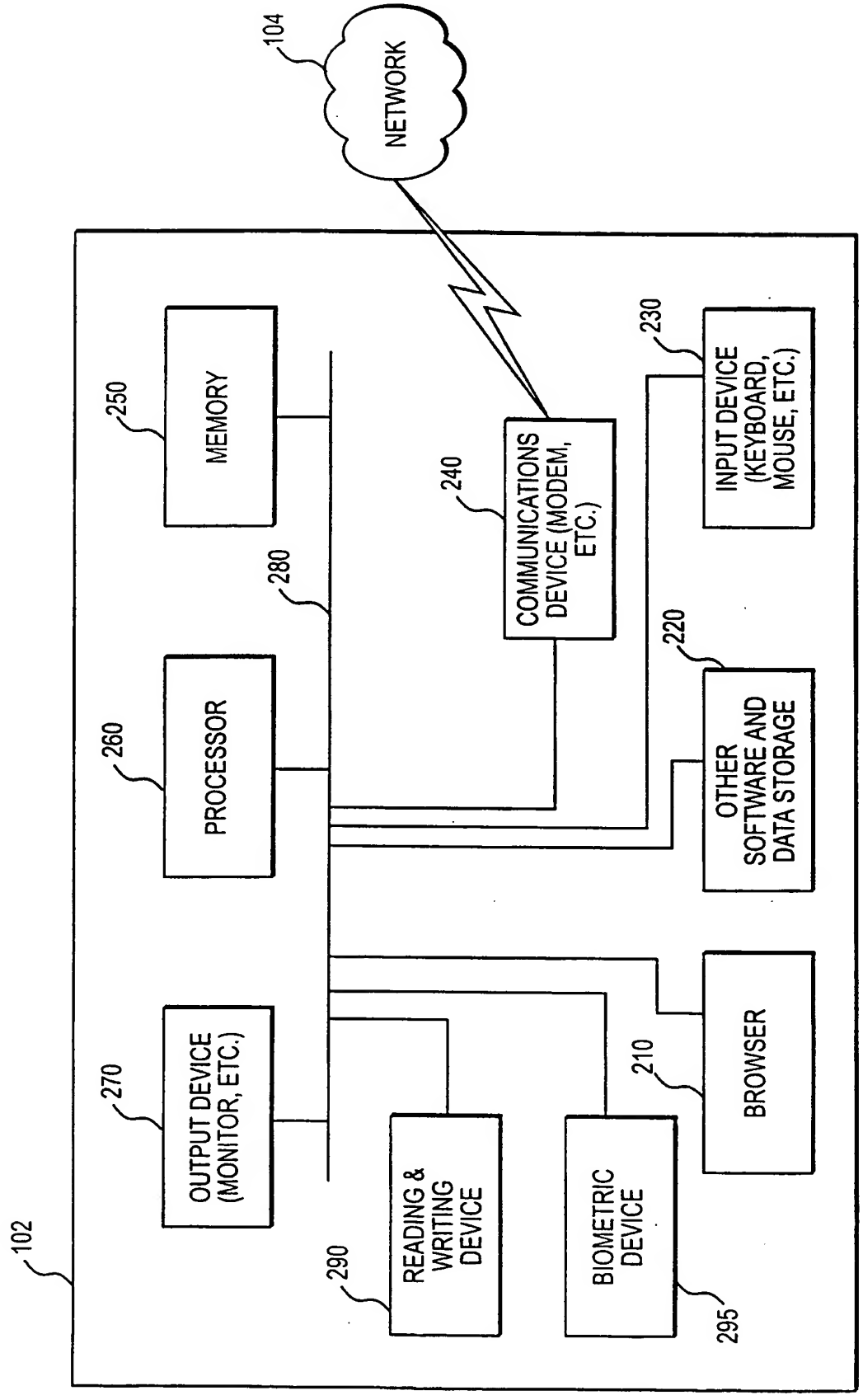

NETWORK
104
MEMORY
250
COMMUNICATIONS DEVICE (MODEM, ETC.)
240
INPUT DEVICE (KEYBOARD, MOUSE, ETC.)
230
280
PROCESSOR
260
OTHER SOFTWARE AND DATA STORAGE
220
OUTPUT DEVICE (MONITOR, ETC.)
270
BROWSER
210
READING & WRITING DEVICE
290
BIOMETRIC DEVICE
295
102

FIG. 2

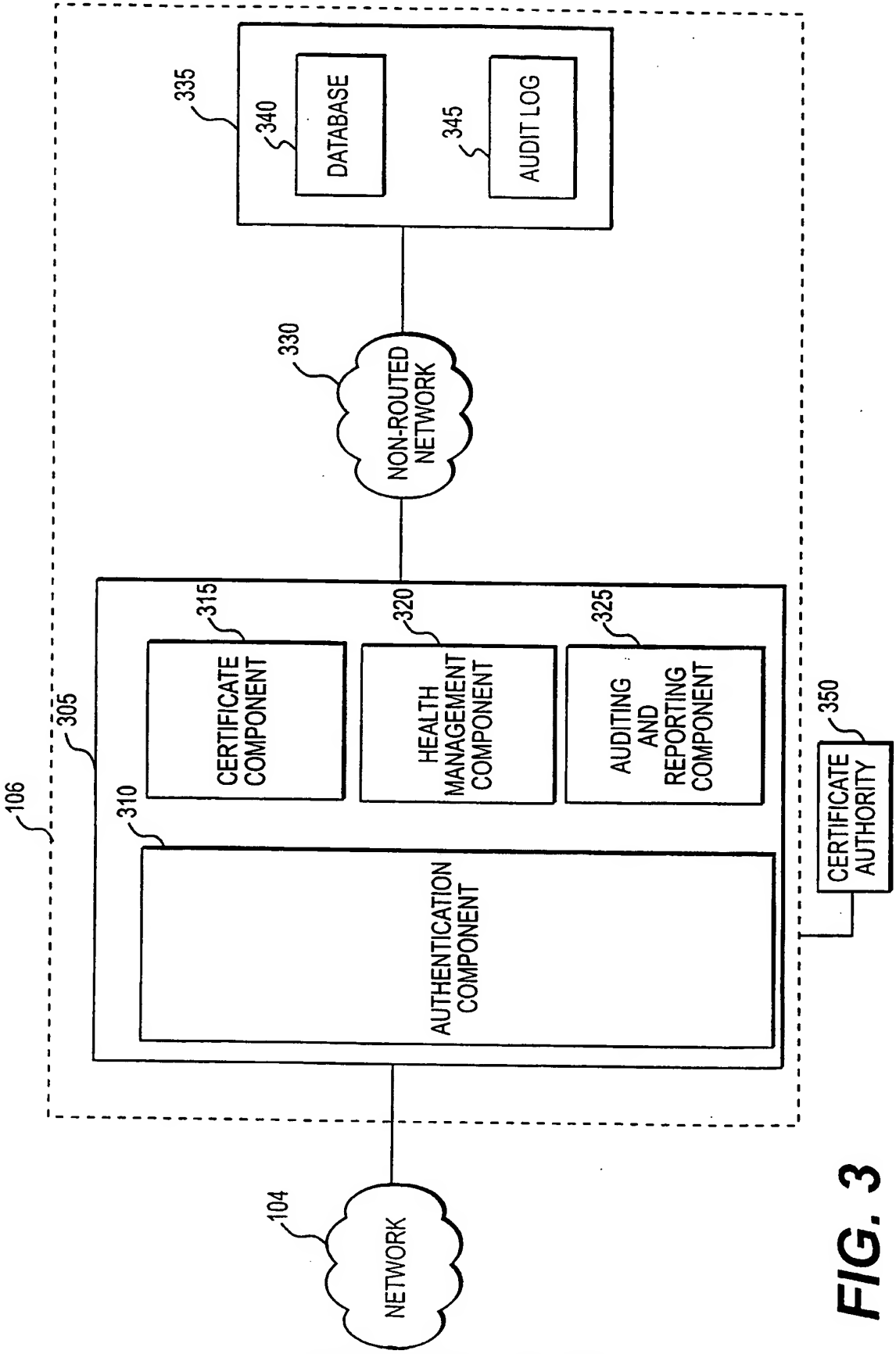

106
305
310
315
320
325
330
335
340
345
350
104
AUTHENTICATION COMPONENT
CERTIFICATE COMPONENT
HEALTH MANAGEMENT COMPONENT
AUDITING AND REPORTING COMPONENT
NON-ROUTED NETWORK
DATABASE
AUDIT LOG
CERTIFICATE AUTHORITY
NETWORK

FIG. 3

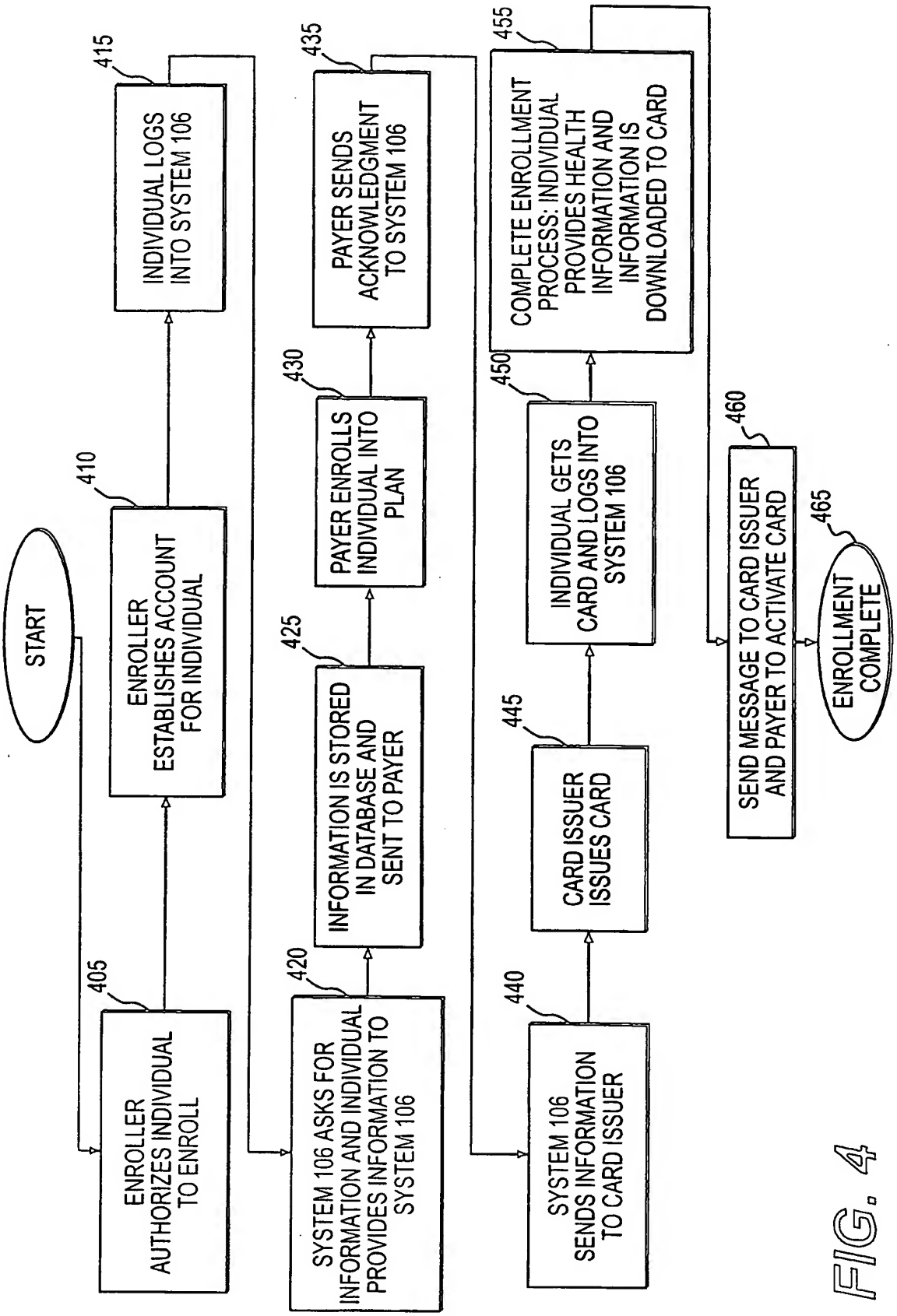

START
ENROLLER AUTHORIZES INDIVIDUAL TO ENROLL
405
ENROLLER ESTABLISHES ACCOUNT FOR INDIVIDUAL
410
INDIVIDUAL LOGS INTO SYSTEM 106
415
SYSTEM 106 ASKS FOR INFORMATION AND INDIVIDUAL PROVIDES INFORMATION TO SYSTEM 106
420
INFORMATION IS STORED IN DATABASE AND SENT TO PAYER
425
PAYER ENROLLS INDIVIDUAL INTO PLAN
430
PAYER SENDS ACKNOWLEDGMENT TO SYSTEM 106
435
SYSTEM 106 SENDS INFORMATION TO CARD ISSUER
440
CARD ISSUER ISSUES CARD
445
INDIVIDUAL GETS CARD AND LOGS INTO SYSTEM 106
450
COMPLETE ENROLLMENT PROCESS: INDIVIDUAL PROVIDES HEALTH INFORMATION AND INFORMATION IS DOWNLOADED TO CARD
455
SEND MESSAGE TO CARD ISSUER AND PAYER TO ACTIVATE CARD
460
ENROLLMENT COMPLETE
465

FIG. 4

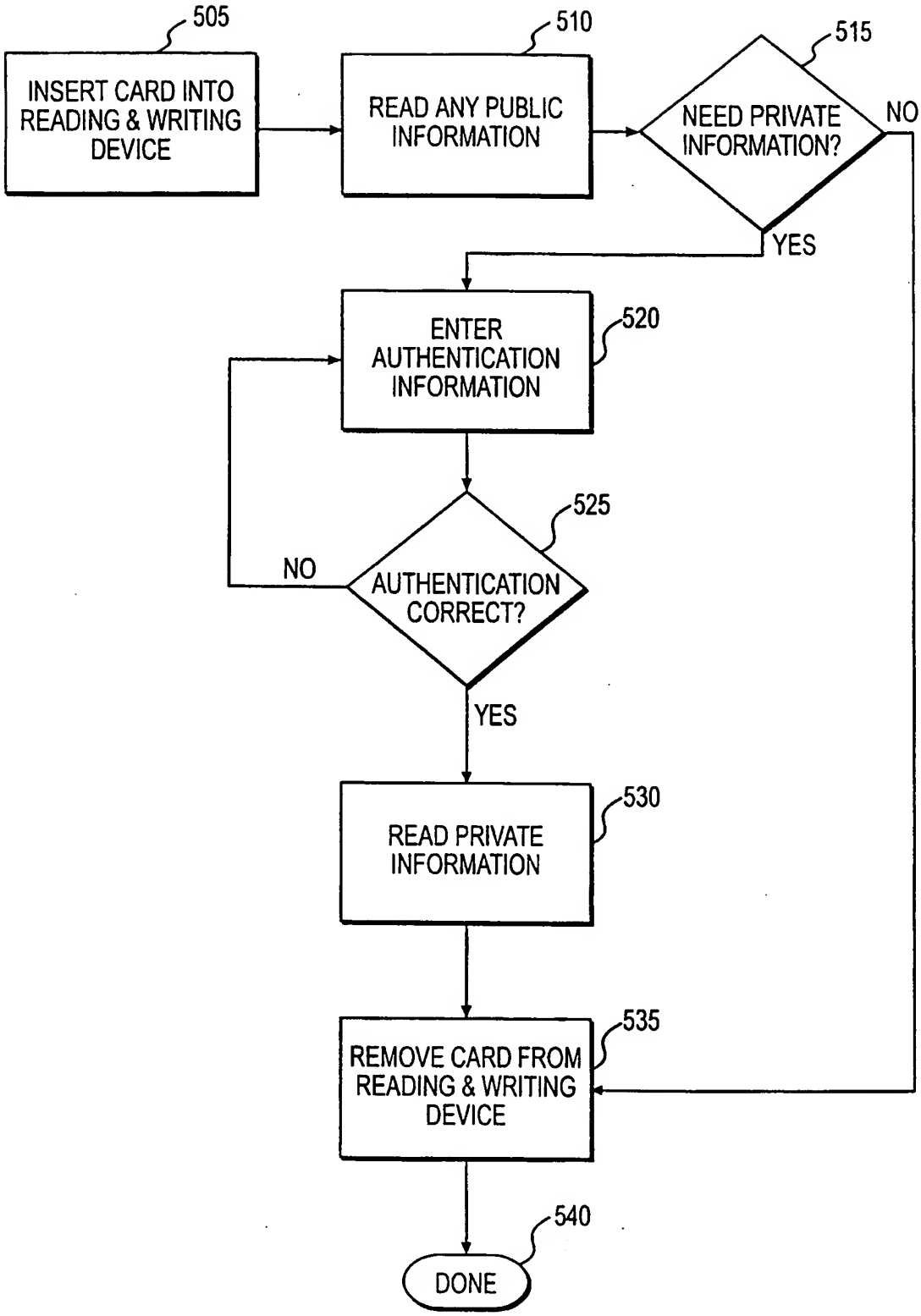

505
INSERT CARD INTO READING & WRITING DEVICE
510
READ ANY PUBLIC INFORMATION
515
NEED PRIVATE INFORMATION?
NO
YES
ENTER AUTHENTICATION INFORMATION
520
525
NO
AUTHENTICATION CORRECT?
YES
READ PRIVATE INFORMATION
530
REMOVE CARD FROM READING & WRITING DEVICE
535
540
DONE

FIG. 5

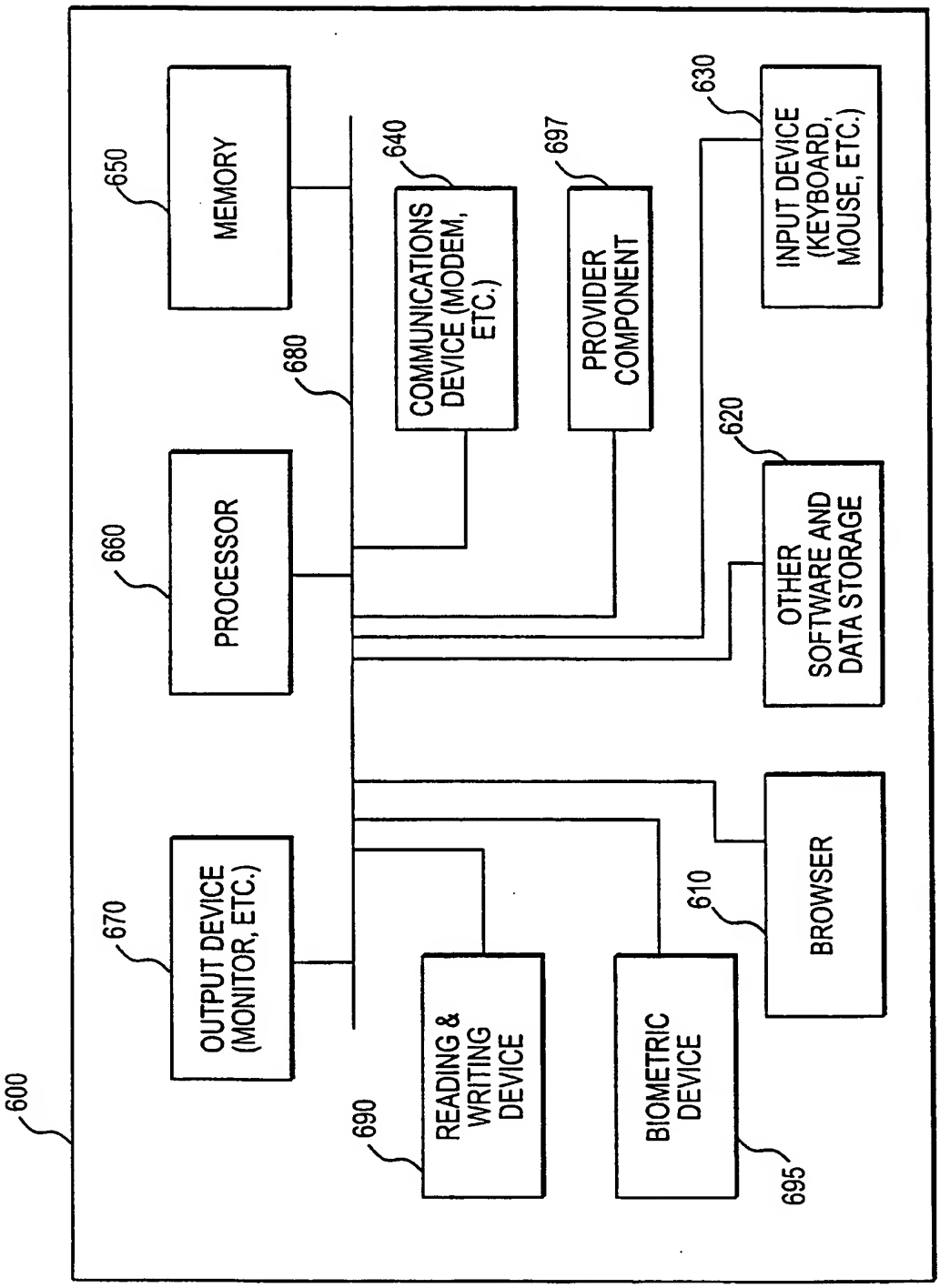

600
MEMORY
650
COMMUNICATIONS DEVICE (MODEM, ETC.)
640
PROVIDER COMPONENT
697
INPUT DEVICE (KEYBOARD, MOUSE, ETC.)
630
680
PROCESSOR
660
OTHER SOFTWARE AND DATA STORAGE
620
OUTPUT DEVICE (MONITOR, ETC.)
670
BROWSER
610
READING & WRITING DEVICE
690
BIOMETRIC DEVICE
695

FIG. 6

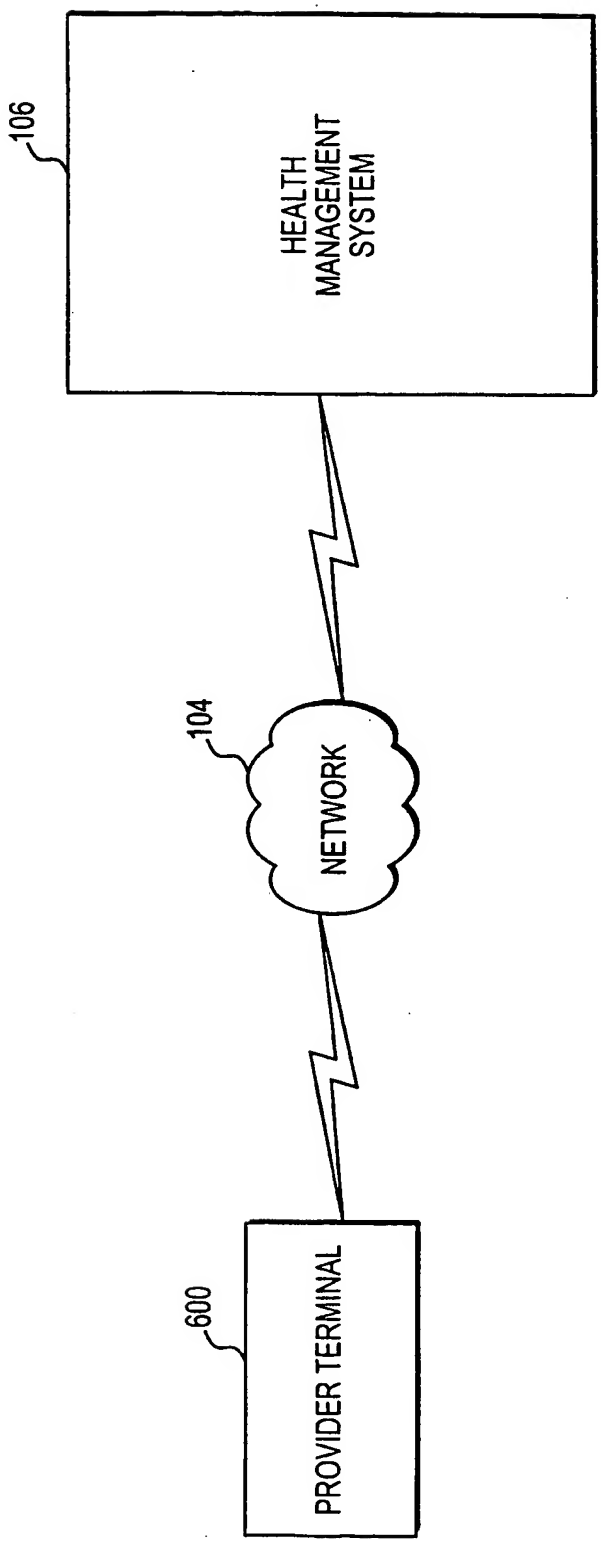

106
HEALTH MANAGEMENT SYSTEM
104
NETWORK
600
PROVIDER TERMINAL

FIG. 7

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 March 2001 (01.03.2001)

PCT

(10) International Publication Number
WO 01/014974 A3

(51) International Patent Classification[7]: G06F 19/00

(21) International Application Number: PCT/US00/23028

(22) International Filing Date: 23 August 2000 (23.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/149,910 23 August 1999 (23.08.1999) US
09/604,727 28 June 2000 (28.06.2000) US

(71) Applicant: **PRESIDEO, INC.** [US/US]; 10305 102nd Terrace, Sebastian, FL 32958 (US).

(72) Inventors: **SCHWEITZER, Shelia, H.**; 171 Shores Drive, Indian River Shores, FL 32963 (US). **LOWTHERS, Bruce, F., Jr.**; 5280-402 W. Harbor Village Drive, Vero Beach, FL 32967 (US). **HOFFMAN, Thomas, C.**; 473 Red Sail Way, Satellite Beach, FL 32937 (US). **FLICKINGER, David, B.**; 1831 Highway A1A #3304, Indian Harbor Beach, FL 32937 (US). **BURKS, James, L.**; 1200 Spanish Lace Lane, Vero Beach, FL 32963 (US).

(74) Agents: **GARRET, Arthur, S.** et al.; Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P., 1300 I Street, N.W., Washington, DC 20005-3315 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

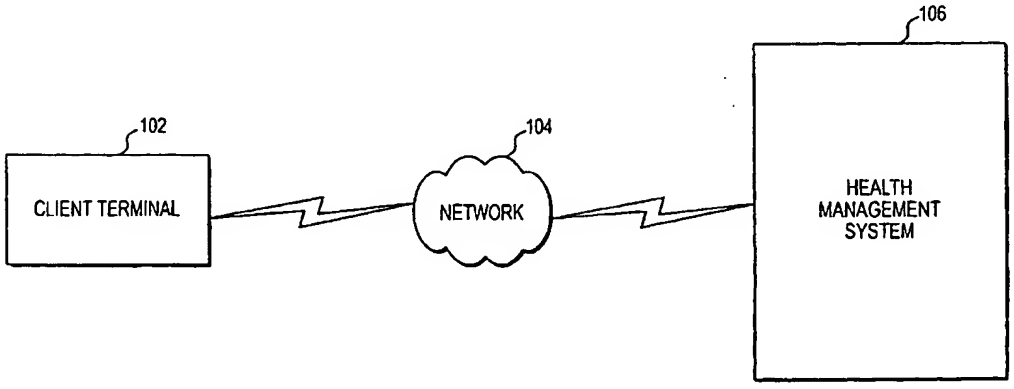
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
11 July 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM, METHOD, AND ARTICLE OF MANUFACTURE FOR IDENTIFYING AN INDIVIDUAL AND MANAGING AN INDIVIDUAL'S HEALTH RECORDS



(57) Abstract: A system, method, and article of manufacture for identifying an individual and managing health records of the individual are provided. The method includes storing health data of an individual on a storage medium. The method also includes logging into the storage medium to manage the health data stored one the storage medium and managing the health data on the storage medium.

WO 01/014974 A3

INTERNATIONAL SEARCH REPORT

Interr "onal Application No
PCT/US 00/23028

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 08755 A (ROST IRMGARD) 21 March 1996 (1996-03-21) page 1, line 6 -page 15, line 28 page 19, line 13 - line 24 page 28, line 28 -page 34, line 21 ---	1-26
A	WO 97 04712 A (MC MEDICAL CARD SYSTEMS GMBH) 13 February 1997 (1997-02-13) page 1, line 1 -page 12, line 5 ---	1-26
A	US 5 499 293 A (BEHRAM SEPEHR ET AL) 12 March 1996 (1996-03-12) abstract column 2, line 27 -column 4, line 40 column 12, line 8 -column 13, line 5 --- -/--	1-26

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 January 2002	23/01/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Schenkels, P

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interr ''onal Application No
PCT/US 00/23028

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 683 465 A (AT & T GLOBAL INF SOLUTION) 22 November 1995 (1995-11-22) abstract ---	22-26
A	WO 93 20538 A (ZUK EDWARD ANDREW ;TELSTRA CORP LTD (AU)) 14 October 1993 (1993-10-14) abstract -----	2,4,5, 12,17

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

..formation on patent family members

Inter ·onal Application No
PCT/US 00/23028

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9608755	A	21-03-1996	AT	163235 T	15-02-1998
			AU	3606795 A	29-03-1996
			CA	2199934 A1	21-03-1996
			DE	19580995 D2	04-12-1997
			DE	59501456 D1	19-03-1998
			WO	9608755 A1	21-03-1996
			EP	0781428 A1	02-07-1997
			ES	2116107 T3	01-07-1998
			JP	10505695 T	02-06-1998
WO 9704712	A	13-02-1997	DE	19536204 A1	30-01-1997
			WO	9704712 A1	13-02-1997
US 5499293	A	12-03-1996	NONE		
EP 0683465	A	22-11-1995	EP	0683465 A2	22-11-1995
			JP	7319971 A	08-12-1995
WO 9320538	A	14-10-1993	AT	207642 T	15-11-2001
			AU	671986 B2	19-09-1996
			AU	3818093 A	08-11-1993
			WO	9320538 A1	14-10-1993
			CA	2133200 A1	14-10-1993
			DE	69331006 D1	29-11-2001
			EP	0634038 A1	18-01-1995
			JP	7505270 T	08-06-1995
			SG	46692 A1	20-02-1998
			US	5745571 A	28-04-1998